

Remarks/Arguments

Claims 1-11 are pending.

Objection to claims 4 and 9 under 35 USC 112, second paragraph

Claims 4 and 9 have been amended in view of the rejection under 35 USC 112, second paragraph, to delete the term "compactflash."

Rejection of claims 1-11 under 35 USC 103(a) as being unpatentable over Boyle et al. (US Pat. No. 6118870) in view of Kato et al. (US Pat. No. 6301993)

Applicants submit that present claims 1-11 are patentably distinguishable over the teachings of Boyle and Kato because the resulting combination still fails to teach or suggest notable features of the claimed invention. Applicants also submit that it is improper to combine Boyle and Kato as suggested because there is no teaching or suggestion in the references to combine them in the manner suggested.

The present invention provides a method and apparatus for preventing unauthorized copying and distribution of digital encoded data, in particular, for preventing a user from making multiple playable copies of audio data files from one removable data storage device, such as the flash memory cards (page 2, lines 2-9). In that regard, the present invention provides a player and method for processing audio data files that encrypts the audio data files in response to a **unique identifier associated with a removable data storage device** and a key stored in a key file of the portable audio player (page 2, line 23 - page 3, line 25). In that regard, present claim 1 recites:

the apparatus adapted to be removably coupled to a **data storage device having a unique identifier**, an audio data file and a decoder file stored therein, a method for processing the audio data file, the method comprising the steps of: ...

generating a third key in response to the second key and the unique identifier;

decrypting the audio data file in response to the third key and the decryption program... (emphasis added)

Claim 6 recites similar features in apparatus form and claim 11 recites similar features in the context of the data storage device. Applicants submit that neither Boyle nor Kato, singly or in combination, teach or suggest such use of a unique identifier associated with the data storage device.

Boyle is primarily concerned with the distribution of protected content between a publisher station and a subscriber station over a digital communications link. (Fig. 1; col. 3, lines 21-35; col. 10, lines 40-44 "*Thus disclosed is a digital communications system that provides for the secure transmission of data. The subscriber station provides security by preventing the compressed data from being accessed. Only the uncompressed data, which is not economical to distribute can be accessed.*")

In that regard, Boyle teaches transmitting encrypted and compressed multimedia data and an encrypted EPLAY program for decrypting and decompressing the multimedia data. The multimedia data and the EPLAY program are decrypted with a decryption key, which is either a symmetric key stored in the subscriber station, or a key derived using a public key/private key pair, wherein the private key is stored in the subscriber station. In either case, the same key is used for decrypting the EPLAY program and the multimedia data, and the key does not appear to have any relation to a unique identifier associated with a data storage device adapted to be removably coupled to the subscriber station.

The Office Action acknowledges that Boyle fails to teach the step of using two separate keys to decrypt the decoder file and the audio data, but cites Kato as teaching the use of a different key to decrypt the audio data. Applicants submit that Boyle not only fails to teach the use of separate keys, but also says nothing in regard to the use of a unique identifier associated with a data storage device adapted to be removably coupled to the subscriber station.

Kato teaches a copy protection apparatus that uses electronic watermark information and key information to provide copy protection for data stored on a

disk. The information is encrypted with a disk key, which is obtained on the decryption system side using the electronic watermark information and a part master key col. 1, line 37 - col. 4, line 22). The disk key is used by the encryption system A to encrypt the audio data sequence, and is obtained and used by decryption system C to decrypt the audio data sequence (col. 7, lines 2-9 "*... the encryption key (disk key) for encrypting the audio data sequence...*"; col. 11, lines 5-14). The portion of Kato cited by the Examiner describes the process for obtaining the disk key Dk (col. 7, line 53 to col. 8, line 35).

However, nowhere does Kato teach or suggest deriving a key for decrypting the audio data file in response to a **unique identifier** associated with a data storage device. Kato describes a multi-step process for obtaining the disk key, but says nothing in regard to the disk key being associated with a unique identifier associated with the data storage device. In view of the above, applicants submit that, even assuming arguendo, that Boyle and Kato are combined as suggested by the examiner, the resulting combination fails to disclose or suggest the feature of deriving a third key in response to a second key and a unique identifier stored in the data storage device. Neither Boyle nor Kato say anything in this regard. Therefore, applicants submit that present claim 1, and the claims that depend therefrom, are patentably distinguishable over the proposed combination.

Further, Applicants submit that the combination of Boyle and Kato still do not teach or suggest the two separate keys to decrypt the decoder file and the audio data. In Boyle, a single key is used to decrypt the multi-media data and the EPLAY program. In Kato, the disk key is used to decrypt the audio data sequence. The disk key of Kato may differ from the key used in Boyle, but neither reference teaches or suggests using **separate** keys to decrypt the decoder file and the audio data. Both references teach a single key in that regard. Therefore, applicants submit that the combination of Boyle and Kato still fail to teach or suggest the use of two separate keys as recited in present claim 1, and thus, claim 1, and the claims that depend therefrom, are patentably distinguishable over the proposed combination.

Applicants submit that present claim 6, and the claims that depend therefrom, and present claim 11, are also patentably distinguishable over the proposed combination for at least the same reasons as those discussed above.

Further, applicants submit that it is improper to combine Boyle and Kato as suggested because nowhere do Boyle and Kato teach or suggest such a combination. In Boyle, the multi-media data and the program that controls the decryption and decompression of the multimedia data are transmitted by the publisher station to the subscriber station. That is, Boyle teaches transmitting two separate pieces of encrypted information, wherein one piece of encrypted information is used to derive a second piece of encrypted information.

By contrast, Kato does not teach or suggest transmitting such two separate pieces of encrypted information. In Kato, decryption unit 12 decrypts the audio data sequence using the disk key, and MPEG decoder 14 decompresses and decodes the decrypted audio data sequence (col. 13, lines 4-10). Decoders for decompressing and decoding data stream encoded using the MPEG standards are well known by those skilled in the art. Kato teaches decompressing and decoding the decrypted audio data using an MPEG decoder, and gives no reason or suggestion why it would be desirable to use an encrypted program to control the operation of the MPEG decoder.

In view of the above, it is clear that the systems of Boyle and Kato operate in different fashion, and there is no teaching or suggestion in either Boyle or Kato to combine the references in the suggested manner. Therefore, applicants submit that the Boyle and Kato should not be combined as suggested and that any such combination constitutes impermissible hindsight reconstruction.

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,
SIN HUI CHEAH



By: Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: January 31, 2005

CERTIFICATE OF MAILING

I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to [Mail Stop Amendment], Commissioner for Patents, Alexandria, Virginia 22313-1450 on:

2/01/05
Date

Linda Tindall
Linda Tindall